REMARKS

Claims 1-17 are now pending in this application. In this response, care has been taken to avoid the introduction of new matter. Favorable reconsideration of the application in light of the following comments is respectfully solicited.

In section 8 of the Office Action, claims 1-17 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,076,060 (hereinafter "Bilchev") in view of U.S. Patent App. Pub. No. 2002/0083330 (hereinafter "Shiomi"). Applicants respectfully traverse.

Bilchev teaches a cipher system that employs a plurality of encipher functional modules, in which a key provides "information which describes the process used to carry out enciphering" (col. 1, lines 11-13). The cipher system operates on data in blocks of bits, passing each block of data in sequence through the plurality of encipher functional modules (*see, e.g.,* Figs. 3 and 11). The broad system for ciphering generic binary data disclosed in Bilchev might be employed in any application seeking to encrypt data.

Shiomi teaches what it calls "an encryption process" for circuit design data. As illustrated in Figs. 5A to 5D, Shiomi combines the original design logic (f_0) with dummy logic (f_1), and permutates their respective outputs (21) to output selectors (22). By supplying the correct "key" (k_0 and k_1), the output selection logic will select the outputs corresponding to the original design logic (*see* Figs. 4 and 5C). Once all of the logic is combined and reduced (*see* Fig. 5D), it becomes difficult or impossible to derive the original design. The output of this "encryption" is a functioning circuit description which can be simulated. However, simulation of the circuit is useless unless one supplies the correct key for the output selectors, thereby yielding the behavior of the original design logic (*see* Fig. 4). However, rather than teaching a

reversible method for encrypting design data and a corresponding method of decryption for recovering the original design data, Shiomi teaches a process that is more accurately described as obfuscation or scrambling.

Claims 1-3, 9, 11, 13, and 15

Claim 1 recites an "intermediate data encrypting means for encrypting *intermediate data generated during a simulation*" and "intermediate data decrypting means for . . . providing . . . decrypted *intermediate data* to the simulation means." Neither Bilchev nor Shiomi teach or suggest these recited elements. Bilchev contains no teaching of "intermediate data generated during a simulation," let alone engaging in encrypting or decrypting any such data. Though page 4 of the Office Action cites portions of Bilchev as analogous to the above elements, the cited portions merely discuss the actions of encryption and decryption *generally*. Such a broad disclosure does not teach or suggest performing such actions on "intermediate data generated during a simulation," as recited in claim 1.

Nor does Shiomi teach or suggest the recited limitations. Though Shiomi discusses performing simulations, its teachings are limited to the broad concept of simulating an "encrypted" design, the verification of simulation results, and imposing limitations on performing executing designs in a simulator (*see* ¶¶ 57-80). There is no teaching of "intermediate data generated during a simulation" in general, let alone a hint or suggestion one might or should encrypt or decrypt such data. Arguably, such an issue would not be of concern for a design that has been "encrypted" as taught by Shiomi, as its process of obfuscation and imposing possible limitations on execution in a simulated environment would seriously frustrate attempts at reverse engineering.

Without a teaching or suggestion of all of the recited limitations, in particular those discussed above, the cited references are unable to sustain a *prima facie* case of obviousness against claim 1. For at least the same reasons, claims 2-3 are patentable, as they depend upon claim 1. For substantially the same reasons, claims 9, 11, 13, and 15, which also recite intermediate data encrypting and decrypting means, are patentable over the cited references.

Claims 4-8, 10, 12, 14, 16, and 17

Claim 4 recites "decrypting supplied circuit information encrypted by a *first* encryption technique," a "stored circuit information encrypting means or encrypting, by a *second* encryption technique, the circuit information decrypted by the supplied circuit information decrypting means," and a "stored circuit information decrypting means for decrypting the circuit information . . . encrypted by the *second* encryption technique." Page 5 of the Office Action asserts that Fig. 3, figure 40a of Bilchev discloses the recited "decrypting . . . information encrypted by a first encryption technique," and that Fig. 3, figure 40b discloses the recited "encrypting means . . . by a second encryption technique." However, Bilchev does not disclose the encryption of a previously decrypted data, and certainly not where different encryption techniques are employed. In the context of combining encryption and decryption activities, Bilchev consistently discusses a first encryption followed by a second decryption – *not* the reverse order. Furthermore, the encryption and decryption in Bilchev are the *same* encryption technique. First, the "cipher system" disclosed by Bilchev, which encompasses both the disclosed encryption and decryption, is a single technique. Second, even if the encryption and decryption might be considered different techniques, they are nevertheless a single technique, as deciphering merely uses the same cipher units as encryption – merely in the reverse order (col. 3,

lines 56-61). For these reasons, Bilchev does not teach or suggest the recited limitations of claim 4. The further teachings of Shiomi do not cure this shortcoming.

Without a teaching or suggestion of all of the recited limitations, in particular those discussed above, the cited references are unable to sustain a *prima facie* case of obviousness against claim 4. For at least the same reasons, claims 5-8 are patentable, as they depend upon claim 4. For substantially the same reasons, claims 10, 12, 14, 16, and 17, which recite similar limitations, are patentable over the cited references.

For the above reasons, Applicants believe that the application is in condition for allowance. Applicants respectfully request the Examiner's favorable consideration as to allowance.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Michael E. Fogarty
Registration No. 36,139

Please recognize our Customer No. 20277 as our correspondence address.

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8000 MEF:EMS
Facsimile: 202.756.8087
Date: December 22, 2006